



Nome del corso e codice: **Framework di cybersecurity (AI06.1)**

Date delle sessioni: 21 aprile 2027

Orari: 09:00-13:30

Sede: CEIDA, Via Palestro 24, Roma | Possibile collegamento da remoto

Competence Center: Digital & AI Transformation

Prezzo: € 450,00 + IVA (la quota è esente da IVA se corrisposta da Enti pubblici)

Docente	Mattia Siciliano
Info di contatto	Mail: segreteria@ceida.com
Orario ricevimento	Appuntamento da concordare via mail

Descrizione del corso

Il Corso esplora i principali rischi di cybersecurity e le sfide che le moderne organizzazioni devono affrontare, con focus sui nuovi scenari creati dall'AI e dall'Internet of Things (IoT). Gli studenti svilupperanno competenze avanzate su aspetti regolatori, tecnici e manageriali. Ci sarà anche spazio per un approfondimento legale simulando situazioni reali.

Obiettivi di apprendimento

Gli studenti acquisiranno conoscenza delle principali forme di attacchi cyber e dei loro impatti sulle organizzazioni, come degli aspetti regolatori, compreso GDPR, Cybersecurity Act, NIS 2. Lavoreranno altresì alle tecniche di mitigazione e di controllo, come Cyber Killchain, analisi di attacchi di superficie, penetration testing. Infine, analizzeranno responsabilità di governance e di board nella cybersecurity.

Target

Il percorso è rivolto a membri di team aziendali e governativi, come a professionisti per un rafforzamento delle competenze.

Programma

Modulo 1: Cybercrime: Data, Scenari, Impatti (AI06.1) – Data: 21 aprile 2027 – Orario: 9:00-13:30

- Evoluzione degli attacchi cyber e delle minacce (phishing, ransomware, data exfiltration, BEC, CEO fraud, SIM swap);
- Framework regolatorio: NIS 2 e legislazione Italiana cybersecurity per il settore pubblico;
- ICT governance, risk management, vulnerability analysis;
- Il fenomeno “Crime as a Service” e ransomware come servizio;
- I framework ISO 27001 and ISO 62443;
- Profili regolatori: GDPR, Cybersecurity Act, ruolo della National Cybersecurity Agency (ACN);
- Multe, ispezioni, danno reputazionale da minacce di cybersecurity;
- Regole nazionali e responsabilità ex Legge 231/2001.

Risorse di apprendimento

Video, case-histories, questionari.

Metodologia di apprendimento

Casi reali, simulazioni di attacchi, guest speaker.

Sintesi del percorso di apprendimento

Sessione	Data	Orario	Docente
Modulo 1: Cybercrime: Data, Scenari, Impatti	21/04/27	09:00-13:30	Mattia Siciliano

Lettere consigliate

- Direttive CAN
- Cybersecurity Act e Direttiva NIS2

Profilo Coordinatore Scientifico

Mattia Siciliano. Ingegnere, cybersecurity expert, con oltre 15 anni di esperienza in progetti internazionali sia con multinazionali sia governativi. Nel corso della sua carriera ha sviluppato un approccio distintivo che integra soluzioni digitali innovative con strategie di difesa. Supporta top management e consigli di amministrazione nella gestione dei rischi legati alle tecnologie digitali ed è attivamente coinvolto in iniziative istituzionali e strategiche in ambito cybersecurity.

Raccomandazione!

Si informa che l'attivazione del corso avverrà esclusivamente a seguito di comunicazione scritta da parte del CEIDA. Pertanto, si sconsiglia vivamente di effettuare prenotazioni o acquisti di titoli di viaggio, pernottamenti o altri servizi connessi, prima di aver ricevuto tale conferma ufficiale, comprensiva della modalità di erogazione del corso (in presenza o a distanza). CEIDA declina ogni responsabilità per eventuali spese sostenute anticipatamente e non potrà essere ritenuto in alcun modo tenuto a rimborsi o compensazioni di natura economica o altra.